Cipher Machines & Cryptology

http://users.telenet.be/d.rijmenants

Ed. 7.4 – Jan 22, 2016

THE COMPLETE GUIDE TO

SECURE COMMUNICATIONS

WITH THE

ONE TIME PAD CIPHER

DIRK RIJMENANTS

Abstract: This paper provides standard instructions on how to protect short text messages with one-time pad encryption. The encryption is performed with nothing more than a pencil and paper, but provides absolute message security. If properly applied, it is mathematically impossible for any eavesdropper to decrypt or break the message without the proper key.

Keywords: cryptography, one-time pad, encryption, message security, conversion table, steganography, codebook, covert communications, Morse cut numbers.

Contents

1. Introduction

One-time pad encryption is a basic yet solid method to protect short text messages. This paper explains how to use one-time pads, how to set up secure one-time pad communications and how to deal with its various security issues. Working with one-time pads is easy to learn. The system is transparent and you do not need a computer, special equipment or any knowledge about cryptographic techniques or mathematics.

One-time pad encryption is an equation with two unknowns, which is mathematically unsolvable. The system therefore provides truly unbreakable encryption when properly used. It will never be possible to decipher one-time pad encrypted data without having the proper key, regardless any existing or future cryptanalytic attack or technology, infinite computational power or infinite time.

It is however paramount to carefully read and strictly follow the security rules and advice, found in chapter 7, to ensure the security of the message. Do not use one-time pads in a real situation before reading this paper from start to end!

A brief history of one-time pad is presented in appendix G (§ 10.7).

1.1 Why should you use encryption?

Cryptography can protect the secrecy of your private communications. Privacy is a natural right that allows personal autonomy, while ensuring your democratic freedoms of association and expression. The definition of privacy differs among cultures and countries. Some governments impose restrictions or prohibit the use of strong cryptography by their citizens because it limits government surveillance. The fight against crime and terrorism are popular excuses to blur the boundary between legally authorized surveillance and blunt intrusion in people's privacy.

Please read chapter 9 for more info about the legal issues regarding the use of cryptography.

1.2 Common notations

Some notations, used in this paper: *cryptography* and *cryptanalysis* are the sciences of making and breaking codes. The readable and unprotected message is called *plaintext*. Plaintext that is encoded into digits is called plaincode (to stress that it is still in plain readable form). *Encryption* or *enciphering* is the process to make a message unintelligible by applying an *algorithm* under control of a key. The result of encryption is called *ciphertext*. *Decryption* or *deciphering* is the process to turn the ciphertext back into readable plaincode or plaintext with the help of the proper key.

2. The One-time Pad

To perform one-time pad encryption we need a key, called one-time pad. A one-time pad can be a single sheet, a booklet or a strip or roll of paper tape that contains series of truly random digits. A one-time pad set consists of two identical one-time pads, one pad called OUT and one called IN.

To establish one-way communications, you only need one OUT pad for the sender and an identical copy called IN pad for the receiver. To communicate in both ways, you need two different one-time pad sets: person A has an OUT pad of which person B has the IN copy, and person B has another OUT pad of which person A has the IN copy. Never use a single pad to communicate in both directions to avoid the risk of simultaneous use of the same pad sheet!

The use of multiple IN copies of a pad, to enable more than one person to receive a message, is possible but not advisable. Multiple copies pose additional security risks and should only be used in a strictly controlled environment. Never use multiple OUT copies of a pad, as this will inevitable result in simultaneous use of the same pad and the risk of non destroyed copies of a pad.

One-time pad encryption is only possible if both sender and receiver are in possession of the same key. Therefore, both parties must exchange their keys beforehand. This means that the secure communications are expected and planned within a specific period. Enough key material must be available for all required communications until a new exchange of keys is possible. Depending on the situation, a large volume of keys could be required for a short time period, or few keys could be sufficient for a very long period, up to several years.

Carefully read the instructions in § 7.2 on creating one-time pads with truly random digits, before making your own one-time pads. This is the most vital part of the message security!

Example of a one-time pad sheet:

```
              OUT 0001

68496 47757 10126 36660 25066
07418 79781 48209 28600 65589
04417 18375 89891 68548 65437
96152 81871 38849 23191 35777
59888 98186 01174 19456 73831
74345 88365 39797 08166 97776
96571 53718 56970 37940 60539
91243 74502 87465 41884 44533
72057 94612 35304 29054 33274
48090 79776 45366 46827 11680

          DESTROY AFTER USE
```

Note that there are also one-time pads with random letters. Such pads are only suitable to encrypt letters-only text. For reasons of flexibility and practicality, the one-time pad system, presented in this paper, uses pads with random digits.

3. Message Preparation

Use short concise sentences and avoid repetitions when composing your message. Omit spaces where it does not affect readability. Use abbreviations where possible. If available, use a codebook to reduce message length (see chapter 6). Do not use names of persons or places if the origin or destination of the message, or the message content clarifies those names or places. Never use a fixed structure or format in the message. The message should not exceed 250 digits after conversion (approx. 180 characters). Split larger messages into parts of 250 digits and encrypt each part with a new one-time pad key.

Before we can encrypt the message, we must convert the plaintext into a series of digits, called plaincode, with the help of a checkerboard. The frequently used letters are represented by a single-digit value. All other characters are represented by a double-digit value. The table is optimised for English. Note that this plaincode on itself provides absolutely no security whatsoever and must always be followed by the proper encryption! More about various checkerboards in §10.1

The character-to-digits checkerboard and its printable version:

CODE 0	A 1	E 2	I 3	N 4	O 5	T 6	CT NO 1 ENGLISH		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	S 83	U 84	V 85	W 86	X 87	Y 88	Z 89
FIG 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	SPC 99

```
 CONVERSION TABLE NO.1 EN

CODE-0  B-70  P-80  FIG-90
   A-1  C-71  Q-81  (.)-91
   E-2  D-72  R-82  (:)-92
   I-3  F-73  S-83  (')-93
   N-4  G-74  U-84  ( )-94
   O-5  H-75  V-85  (+)-95
   T-6  J-76  W-86  (-)-96
        K-77  X-87  (=)-97
        L-78  Y-88  REQ-98
        M-79  Z-89  SPC-99
```

Spaces are represented by 99 (SPC). A comma and apostrophe are both represented by 93 (') and 94 ( ) opens and closes parentheses. Figures are always written out three times to exclude errors and they are preceded and followed by 90 (FIG). If required, the Request code 98 (REQ) can be replaced by a question mark. Punctuations are allowed within figures. Some examples:

```
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N     N  Y  (.)
79 2  2  6  3  4  74 99 1  6  90 111 444 90 80 79 99 3  4 99 4  88 91

S  I  Z  E  =      3   .   5     F  E  E  T
83 3  89 2  97 90 333 91 555 90 73 2  2  6
```

The codebook prefix CODE (0) precedes three-digit codebook values. Spaces are unnecessary before and after codebook codes. The use of a codebook is optional but can reduce the message length and transmission time considerably. You can always omit the use of a codebook if the receiver does not posses a copy of the codebook.

In the next example, we use the codebook values PASSPORT (587), FLIGHT (352), UNABLE-TO (884) and FERRY (343) from the codebook in chapter 6.

```
REQUEST  N E W  PASSPORT  F  O R  FLIGHT (.) UNABLE TO  U  S  E  FERRY
98       4 2 86 0587      73 5 82 0352   91  0884       84 83 2  0343
```

Notice that we only need 34 digits for a text with 43 characters, which is a very efficient 0.8 digit/letter ratio, compared to an average 1.3 ratio in a text conversion without codebook.

4. Encryption

Before we start the encryption process, we must tell the receiver which one-time pad is used. Therefore, the first group of the one-time pad is used as key indicator at the beginning of the message. Never use the first group of the pad in the encryption process! Never send a one-time pad serial number along with the message because this would reveal the number of messages that were sent, and their order.

To encrypt the message, write down the plaincode digits of the converted text in groups of five digits and write the digits of the one-time pad underneath them. Always complete the last group with full stops (9191…). Do not forget to skip the first group (key indicator) of the one-time pad!

Subtract the one-time pad digits from the plaincode, digit by digit, from left to right and by modulo 10. This means subtracting without borrowing (e.g. 5 - 9 = 6 because [1]5 – 9 = 6 but we do not borrow that [1] from the next left digit!). Never perform a normal subtraction because that will create a biased and completely insecure ciphertext!

In the following example, we use the one-time pad key from chapter 2 and the plaintext message from chapter 3.

```
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N     N  Y  (.)
79 2  2  6  3  4  74 99 1  6  90 111 444 90 80 79 99 3  4 99 4  88 91

Plaincode : KEYID 79226 34749 91690 11144 49080 79993 49948 89191
OTP Key(-): 68496 47757 10126 36660 25066 07418 79781 48209 28600
            -----------------------------------------------------
Ciphertext: 68496 32579 24623 65030 96188 42672 00212 01749 61591
```

Below, the complete ciphertext, rearranged in the standard format of five groups per row. If the message is sent by radio, in voice or Morse, or by telephone, it is recommended to relay all groups twice to avoid errors (e.g. 68496 68496 32579 32579...). If the receiver has the call sign 401, the message might look like this:

```
401 401 401

68496 32579 24623 65030 96188
42672 00212 01749 61591
```

Important:

- Always encrypt each new message with a new sheet. Never reuse a pad!
- Always destroy the complete one-time pad sheet immediately after finishing the encryption, even when it still contains unused groups.

5. Decryption

To decrypt the message, check its first group (the key indicator) against the first group of your one-time pad to make sure that the proper one-time pad is used. Remember that this first group is not part of the actual message and only serves as key indicator.

Write the one-time pad digits underneath the ciphertext and add ciphertext and one-time pad together, digit by digit, from left to right and by modulo 10. This means addition without carry (e.g. 9 + 6 = 5 and not 15). Never use normal addition!

```
Ciphertext: 68496 32579 24623 65030 96188 42672 00212 01749 61591
OTP Key(+): 68496 47757 10126 36660 25066 07418 79781 48209 28600
            -----------------------------------------------------
Plaincode : KEYID 79226 34749 91690 11144 49080 79993 49948 89191
```

After decryption, the resulting plaincode digits are re-converted back into plaintext with the help of the checkerboard. It is easy to separate the single-digit from the double-digit values: if the first-next digit is between 1 and 6, it represents a single-digit value. If the first-next digit is 7, 8 or 9, it represents a double-digit value and we have to append the following digit to complete the double-digit value. If the next digit is 0 (CODE), it will be followed by a three-digit code that represents a word or expression from the codebook. Remember that figures were written out three times.

Our message, re-converted into text with the checkerboard:

```
79 2  2  6  3  4  74 99 1  6 90 111 444 90 80 79 99 3  4 99 4  88 91
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N    N  Y  (.)
```

Written out: MEETING AT 14 PM IN NY

Important: always destroy the one-time pad sheet immediately after decryption!

Encryption & Decryption Quick Summary

To encrypt, convert the message into plaincode digits and subtract, without borrowing, the one-time pad from the plaincode. Skip the first group of the one-time pad during the encryption process and use it as key indicator at the beginning of the ciphertext.

To decrypt, verify whether the first group of the ciphertext (key indicator) is identical to the first group on your one-time pad. Write the one-time pad underneath the ciphertext digits and add both together without carry. Convert the resulting plaincode with the checkerboard table back into readable text.

ALWAYS DESTROY THE ONE-TIME PAD IMMEDIATELY AFTER USE!

NEVER USE A ONE-TIME PAD MORE THAN ONCE!

PERFORM ALL CALCULATIONS DIGIT BY DIGIT AND MODULO 10 (WITHOUT CARRY OR BORROWING)

6. The Optional Codebook

The codebook table no. 1 (see also §10.2-5) contains various words that would normally require more than four digits to convert. The words are listed in alphabetic order. The non-consecutive values are selected carefully in order to detect single-digit errors and in most cases double-digits errors during decryption (an error results in a non-existing value). The codes 947 through 992 are available for local geographical names, specific technical expressions or names. The codebook prefix CODE (0) must precede each codebook value!

CODE TABLE NO.1

000	ABORT	253	DECODE	505	MILITARY	758	STREET
019	ACCEPT	262	DELAY	514	MONEY	767	SUBWAY
028	ACCESS	271	DIFFICULT	523	MONTH	776	SUCCESS
037	ADDRESS	280	DOCUMENT	532	MORNING	785	SUPPLY
046	AFFIRMATIVE	299	ENCODE	541	MORSE	794	SUPPORT
055	AGENT	307	EVENING	550	NEGATIVE	802	TELEPHONE
064	AIRPLANE	316	EXECUTE	569	NIGHT	811	TODAY
073	AIRPORT	325	FACTORY	578	OBSERVATION	820	TOMORROW
082	ANSWER	334	FAILED	587	PASSPORT	839	TRAIN
091	AUTHORITY	343	FERRY	596	PERSON	848	TRANSFER
109	BETWEEN	352	FLIGHT	604	PHOTOGRAPH	857	TRANSMIT
118	BORDER	361	FREQUENCY	613	POSITIVE	866	TRAVEL
127	BUILDING	370	HARBOUR	622	POSSIBLE	875	TRUCK
136	CANCEL	389	HELICOPTER	631	POWER	884	UNABLE TO
145	CHANGE	398	HIGHWAY	640	PRIORITY	893	URGENT
154	CIVILIAN	406	IDENTITY	659	PROBLEM	901	VERIFY
163	COMPROMISE	415	IMMEDIATE	668	QUESTION	910	WEEK
172	COMPUTER	424	IMPOSSIBLE	677	RADIO	929	WITHIN
181	CONFIRM	433	INFORMATION	686	RECEIVE	938	YESTERDAY
190	CONTACT	442	INSTRUCTIONS	695	RENDEZVOUS	947	....
208	COORDINATE	451	LOCATE	703	REPEAT	956	....
217	COUNTRY	460	LOCATION	712	RESERVATION	965	....
226	COVERT	479	MAIL	721	ROUTINE	974	....
235	CURRENT	488	MEETING	730	SATELLITE	983	....
244	DANGER	497	MESSAGE	749	SHIP	992	....

Some words in the codebook are extendable or changed by addition of one or more characters with the help of the checkerboard: the plural of 0596 (PERSON) will be 059683 (PERSONS). The past perfect of 0686 (RECEIVE) will be 068672 (RECEIVED), and 0901 (VERIFY) will be 090172 (VERIFYD or verified). Words can also get another meaning. 0686 (RECEIVE) becomes 068682 (RECEIVER), 0857 (TRANSMIT) becomes 085782 (TRANSMITR or transmitter) and 0226 (COVERT) becomes 02267888 (COVERTLY).

Of course, you can create a codebook with your own words, phrases or expressions, tailor-made to your specific needs. Maintain the special codebook number sequence in order to preserve the error check ability. It is not recommended to use consecutive values (001, 002, 003 …999) because a single-digit error during communications or decryption would produce a completely different codebook word or phrase. Customizable codebooks for 100 and 220 words or phrases, and a codebook number sequence for 807 words and phrases to create a large codebook are found in §10.3-5. All codebook number sequences are composed in such way single-digit errors, and in most cases double-digit errors, are easily detected. Do not forget the prefix CODE (0).

7. Security Rules and Advice

One-time pad encryption seems simple and straightforward, but there are several important rules that are essential for the security of the message. Not following these rules will always result in the compromise of the message and the one-time pads. Even a small and seemingly insignificant mistake can result in unauthorized decryption of the messages. These rules are not negotiable!

History, court documents and intelligence records have shown many examples of intercepted and decrypted one-time pad communications. Such cases are often mistakenly referred to as cases where one-time pads were broken. In reality, those messages were not actually broken but compromised because somebody at some point did not follow the rules. Often, the users were thoroughly instructed beforehand but they believed that those little details did not matter. They were wrong and paid dearly for their negligence!

However, a one-time pad encrypted message is truly unbreakable if the rules are followed. It will always be and always remain unbreakable, even for the brightest cryptologists with the fastest super computers until the end of times, simply because it is mathematically impossible to break one-time pad. Absolute security is a reason to opt for one-time pad. However, safeguarding that level of security is not without effort. Read the following information carefully!

7.1 Using Personal Computers for Cryptographic Operations

The improper use of computers for cryptographic applications is the most common and fatal error. Normal computers are NEVER suitable for crypto applications, despite many commercial firms selling crypto software for personal computers. Only dedicated computers, stored on a secure locations, or special purpose devices are suitable for cryptographic purposes. There is no such thing as a secure personal computer, tablet or smartphone. Those who contradict this either have no clue about security or have a hidden agenda (commercial profit, surveillance…).

The one-time pad system should be used with nothing more than a pencil and paper, and for good reasons. There are some critical security issues to consider when a computer or other peripheral devices are used. Readable data can, and most often will reside unintentionally on computers, in their memory, in temporary or swap files on the hard disk, or in memory buffers of peripherals. No single network connected computer is secure and will always be vulnerable to malicious software, spy ware or intrusion by skilled hackers or professional organisations.

If an eavesdropper cannot decrypt it, he will definitely try to retrieve it from the targeted computer, either remotely by spy ware, by hacking into the computer, or physically by (surreptitious) examination of the computer or its peripherals. He will get the data before encryption or, when already encrypted, by analysing the hard disk for data remanence after encryption. Secure file deletion software can remove (wipe) remanent data by overwriting it. Some well know software are WIPE or ERASER.

Nonetheless, court documents of espionage cases revealed that sensitive data has been recovered successfully from computers, despite wiping software (malfunctioning or poorly performing software, incorrect or negligent use). In 95 percent of the cases, intelligence agencies don't even bother trying to decrypt data. They simply retrieve the readable data from the computer before encryption, without the targeted person ever noticing.

It is essential that you always use a dedicated stand-alone computer (preferably a small laptop or netbook) that is never connected to a network (disable its wifi). If possible, remove its network card and lock the casing. The computer must be stored permanently in a physically secure place (e.g. safe, armoured room) to restrict unauthorized persons from accessing the computer.

As you can see, there are enough reasons not to use a computer: the security measures are difficult to apply, expensive and not full proof. Since one-time pad encryption is most suitable for a small volume of message, it is recommendable to generate the one-time pads and perform encryption and decryption manually.

7.2 Creating One-time Pads

A standard one-time pad consists of a single sheet or a booklet with many different sheets. You need one set of two identical pads for one-way communication and two different sets of two identical pads for two-way communication. Each sheet contains 250 digits, formatted in five-digit groups, which is enough for a message of some 180 characters. All digits must be truly random. This randomness is essential for the security of the encryption process!

The first five-digit group on each single sheet serves as key indicator. Therefore, to avoid confusion or mistakes, one must assure that this key indicator group, apart from being truly random, always differs from the first group of all another sheet in that same pad. Never use a serial number or other pre-arranged format as key indicator, because this would reveal the number of messages already sent, their order or, if the remaining pad sheets are seized, link its owner to previously sent messages.

There is also a more economical format of pads where a single pad is used for many different messages, of course without ever re-using the same numbers. Such pad is a single sheet with a large number of rows, each containing, say, ten five-digit groups. The first group of the first row serves as key indicator and all following groups are used for encryption. After encryption, only the used rows, including partially used rows, are cut from the top of the pad and destroyed. The remaining next rows are used for the next messages, again with the first group as key indicator. This way, only actually used rows, rather than a whole pad, are consumed for one short message.

When a truly random key digit is subtracted from a plaintext digit by modulo 10 (without borrowing) then each resulting ciphertext digit will also be truly random. Consequently, there is no relation between the individual random ciphertext digits, and the ciphertext doesn't reveal any information whatsoever about the plaintext or about other parts of the ciphertext. The process is mathematically irreversible without the proper key.

THE SECURITY DEPENDS ENTIRELY ON THE QUALITY OF THE RANDOMNESS

Do not use nor derive digits from a phone book, technical publications, books, websites or from any series of digits that is printed or published in any form, on any carrier, anywhere. These are all but random, and certainly not secret. Do not use values that are not within the range 0 through 9. Humans are not suitable to produce randomness. They unconsciously behave according to well-defined rules. If they think, “I should not pick a 6 because I already just wrote a 6”, the next digit is not random, because it has followed a rule. Do not just pick some digits for a key.

There are various ways to generate series of truly random digits. The most practical option to generate large quantities of random is a hardware-based true random number generator (TRNG) of which the output is derived from a random noise source. These are available as PC card or as USB device. Only purchase such generators from well-known independent firms. Today, some microprocessors have included a hardware true random generator, using thermal noise or variations in electrical characteristics of the electronic components on the processors. In such case, the computer itself can provide quality randomness, at least when not compromised by the manufacturer on request some government agency! Computers should always be used with caution as they create various complex security risks (see also §7.1).

If you generate random digits purely with software, you will *never* have truly random digits, which is one of the conditions for unbreakable encryption! A computer program will always be deterministic and by definition predictable. If you do want to use a software-based generator, use only a crypto-secure random number Generator (CSRNG), initialised with a very large random seed, derived from a random source like mouse movements and random process time measurements. Again, this last option could produce a cryptographically secure series of digits that is practically unbreakable, but will never be theoretically truly unbreakable.

If you have to encrypt a low volume of messages, you can generate a small number of one-time pads manually. Although time consuming, it is easy to obtain a high quality of randomness. One method is to use five ten-sided dice. Each new throw gives a new group of five truly random digits. Ten-sided dice are available in many toy stores. Never simply use normal six-sided dice by adding the values of the two dice. This method is statistically completely unsuitable to produce values ranging from 0 to 9 and thus absolutely insecure (the total of 7 will occur about 6 times more often than the total 2 or 12).

Instead, use one black and one white die and assign a value to each of the 36 combinations, taking in account the order and colour of the dice (see table below). This way, each combination has a 1/36th or .0277 probability. We can produce three series of values between 0 and 9. The remaining 6 combinations (with a black 6) are simply disregarded, which doesn't affect the probability of the other combinations.

GENERATING TRUE RANDOM DIGITS 0 TO 9
WITH BLACK AND WHITE DICE

BW	BW	BW	BW	BW
11 = 0	21 = 6	31 = 2	41 = 8	51 = 4
12 = 1	22 = 7	32 = 3	42 = 9	52 = 5
13 = 2	23 = 8	33 = 4	43 = 0	53 = 6
14 = 3	24 = 9	34 = 5	44 = 1	54 = 7
15 = 4	25 = 0	35 = 6	45 = 2	55 = 8
16 = 5	26 = 1	36 = 7	46 = 3	56 = 9

THROWS WITH BLACK 6 ARE DISCARDED

Another also time consuming method is a lotto system with balls that are numbered from 0 to 9. Make sure to mix an extracted ball again with the rest of the balls before extracting a new ball.

7.3 Storage of One-time Pads

One-time pads are usually printed as small booklets that contain a large numbers of one-time pad sheets. The top sheet is torn off and destroyed after a message has been encrypted. The pads are printed in various formats and sizes. If both sender and receiver can store their pads securely, these will be normal sized booklets. When used in covert circumstances, the most practical pads are printed with a very small font (font size 4 or less) on very small thin paper sheets. These are easy to hide and destroy, although one should be very careful when hiding them (see also § 7.6).

One-time pads can be stored in tamper-proof sealed containers (plastic, metal or cardboard) to prevent, or at least detect, unauthorised disclosure of unused series of digits. It is not advisable to store one-time pads on a computer, memory stick or CD. Erasing data on these carriers is very problematic and total destruction of used one-time pads is never guaranteed. Specialized techniques exist to retrieve computer data, even after deletion or overwriting. In critical situations, it is harder to quickly dispose or destruct a memory stick, floppy disk or compact disk than to, for example, eat a small paper sheet.

Always distribute the one-time pads physically, either personally or by a trusted courier. Never send one-time pads electronically because there are no means of communication that provides the same level of security. Encryption with a strong crypto algorithm, prior to sending them electronically, is useless and will compromise the one-time pads. Doing so will lower the pad's security from unbreakable down to the security of the used encryption.

The most important part of the one-time pad scheme is a secure key management. If the key is not compromised, the message is mathematically unbreakable. It is clear that those who are responsible for creating and handling one-time pads should be subjected to the highest level of security screening. The number of persons who are responsible for generating the key material should be limited to an absolute minimum.

Immediately after creation, a one-time pad key pair must be serialised and registered. There should be a centralised (star topology) registration and distribution in order to know who has what keys where and when. If a key pad is used, revoked or compromised, the distributor or user must immediately inform all affected parties and all remaining copies of that key must be destroyed immediately. Never use a one-time pad more than once! If you do so, basic cryptanalysis will break all messages, encrypted with the reused one-time pad.

Of course, one-time pad encryption does not always have to be that complicated. It is also very suitable for one-time occasions. Although you normally might never need encryption, you could encounter an emergency where you need secure communications, by telephone, e-mail or regular mail. A lost PIN code during the holidays, someone needs access to the safe in your office or your home burglar alarm needs a reset code. Everyone remembers a situation where he had to give some information but felt uncomfortable with using a phone, a letter or e-mail.

One-time pad encryption offers a solution to convey sensitive information in such one-time situations. You only have to carry a single small emergency one-time pad for one-time use. Of course, you also need a confidant, a family member or employee, who also has a copy of that pad. The pad could contain a small set of random digits and a little checkerboard. Printed in a font size 3 or 4, the pad would measure a mere one by one inch. You could seal it in plastic, store the pad in a medallion, safely hanging on your necklace, or inside your watch, underneath the back cover. In case of emergency, you call home, let them write down a few groups of digits and tell them to get the pad. No elaborate and complicated security measures are involved.

7.4 Compromise of one-time pads

The compromise (no longer being secure) of a one-time pad or a booklet will endanger all communications, made with those one-time pad sheets. Therefore, it is essential to destroy sheet is immediately after used, to prevent the compromise of those messages that are already sent.

A one-time pad (and any related message) is always compromised when:

- used more than once
- not destroyed after use
- not securely stored at any moment in the past.
- a user is suspected to have violated security rules
- exposed intentionally or unintentionally to other people
- lost or no proof of proper destruction
- it is unknown whether the one-time pad is compromised or not

Never use a compromised one-time pad and always notify all users of compromised pads to destroy those pads immediately!

7.5 Secure Encryption and Decryption

Never use a computer to type a plain message or to encrypt or decrypt a message. Instead, use a single piece of paper on a hard surface to write down the message and perform the calculations. Keep in mind that writing on the first page of a bloc note, or on a sheet of paper, placed on top of a magazine or newspaper, always leaves minor impressions on the underlying paper.

Check you encryption before sending the message. A single error could make the message unreadable or result in critical mistakes during decryption. Destroy that paper and the used one-time pad key immediately after you finished. The most secure and convenient method to destroy paper based keys is simply to burn them. Once encrypted, you can store the ciphertext anywhere you like. It will stay unbreakable. However, for reasons of deniability, it is not recommended to store ciphertext on a computer or any other easily accessible medium.

7.6 Message Security

Unbreakable encryption alone does not provide absolute message security. Message security indeed involves secure encryption but also includes various measures that prevent the opponent to retrieve information that helps him to decrypt the message.

If sender and receiver are in a safe environment, free from risk of surveillance, intrusion of the privacy or prosecution, they can send their encrypted communications by any means, even insecure. It does not matter if someone intercepts the encrypted message. The message is unbreakable anyway. Unfortunately, this ideal world hardly exists. Since it is mathematically impossible to break a one-time pad encrypted message by cryptanalysis, any eavesdropper will try to get his hands on either the original readable message or the one-time pad key, used to encrypt that message.

In the real world, the eavesdropper will attempt to retrieve the identity and location of sender or receiver. Identification of the involved persons is the first step in reading their communications. The mere identification of a person who sends or receives encrypted communications, even unintelligible, might have serious consequences under an oppressive regime. Once identified, the eavesdropper can start surveillance and use technical means to retrieve information from that person's computer or perform a surreptitious search of his house to copy unused one-time pads. The person might never know that his one-time pads were compromised and his future messages are going to be read.

The message itself, even unintelligible, might give clues about who is sending the message, about its contents and to whom it was sent. This technique is called traffic analysis. The amount of messages, their length or sudden change in length might link that message to a particular event that occurred prior to, or after the message was sent, leading to the involved persons. To avoid traffic analysis, you can send each message with a fixed length of 250 digits by simple appending the unused random one-time pad digits at the end of the ciphertext. Any eavesdropper would observe that all messages have the same length and he has no idea of the actual message length.

Of course, physical security is also part of message security. If a – surreptitious - house search, theft or seizure are likely or possible, then any document, computer or any other data carrier that contains one-time pad keys, readable messages, ciphertexts, codebooks or instructions should be well hidden or stored on a remote location, impossible to detect by surveillance or a house search. Again, miniature paper one-time pads have the advantage over digital carriers that they are easy to hide. Tiny and thin sheets could be stored anywhere, inside a power socket, in a TV remote control, a pen, inside toys or between layers of a book cover. One's imagination is the limit.
In event of an expected search, they are easily destroyed by burning them. If you hide one-time pads, you should always use some system to detect the compromise of the hiding place. This

could be a very accurate positioning of the pad in the hiding place, or the use of some tiny object (hair, grain of sand or dust particle) that is moved accidentally by the ignorant intruder.

This is a good moment to explain that in case the use of one-time pads is suspected, a house search could mean the total and thorough dismantling of the house and every single object inside, up to the tiniest parts of furniture, coffee machines or even the removal of all plaster on the walls, to mention a few. This sounds funny, unless you are innocent… or when you actually hide pads.

Also, never talk in public about the fact that you use one-time pad encryption and never mention the words “one-time pad”. Select one or more code words to refer to one-time pad communications. Tell your friend to bring along some “*marshmallows*”, or to send you a new ‘*baseball cap*”. Do not call him by phone and tell him you ran out of one-time pads.

Now that we understand the ways in which our manner of communication influences message security - along with our personal security - we can take measures to avoid detection of our communications.

7.7 Covert Communications

If the opponent has the technical means for surveillance, we need to communicate covertly or disguise our message. Covert communications are a most difficult issue. Telephone, mobile or satellite phone, voice or text message, paper mail, e-mail, the Internet and other network based digital communications are always to be considered absolutely insecure. They enable identification of both sender and receiver. These channels should never be used to communicate covertly.

Today, all digital communications are stored for longer periods. A phone call or cell phone's text message are no longer moments in time. These are digital events, permanently residing in databases, ready to be exploited. An anonymously bought pre-paid card will link a particular cell phone or phone boot to a call or text message. If the pre-paid card or cell phone, used for covert communications, are reused for other purposes, it will be possible to link both events and, combined with geo-location, can lead to both participants of the call. Be aware that the trick of breaking off the conversation before they can trace you is Hollywood fantasy in today’s digital world. A call is traceable from the very first second, even years after the call ended, just as e-mail traffic is. All these cards, phones and Internet connections are only suitable for one-time use.

Publicly available systems could be suitable to communicate anonymously. Some examples are computers in a cyber café or library (of course without need for registration) or a public phone (with anonymously bought pre-paid card). We can post or read message on Internet forums or on random on-line guest books, with a cyber-café computer. However, although publicly available communications might be anonymous, it remains possible to retrieve time and location of these communications. In such case, a witness or security camera could link that particular time and place to the user of that public phone or computer.

Shortwave radio is an ideal way to receive messages covertly over large distances, either by voice, by Morse or a modulated signal which could requires special equipment or software. Morse code is a most suitable method to convey the message digits. It enables good reception, even under very poor conditions, and it is easy to learn. If the message contains only digits, the use of so-called *cut numbers* can reduces the transmission time considerably (see §10.6).

Having a simple household shortwave radio is not suspicious in most countries. Of course, one must avoid storing the receiving frequency in the radio preset memory or its “last used frequency” memory. Although technically possible, it is difficult to locate someone who receives a particular broadcast. Receivers use local oscillators to tune to the desired frequency, and these oscillators unintentionally emanate weak spurious signals. These signals are traceable only with very sensitive equipment in the vicinity of the receiver. Nevertheless, it is a good habit to keep distance, something that might be difficult in cities or buildings where surveillance nearby is possible.

Sending a message covertly with a radio transmitter poses more risks. A broadcast can be located within seconds if the opponent has the proper direction finding equipment. The current SDR technology permits surveillance and interception of many signals simultaneously on several wide frequency ranges. The use of burst-transmission (transmitting a message at high speed) might not be sufficient to avoid detection. Therefore, a radio broadcast is only suitable when the transmitter is located out of the opponent's reach. Another possibility is to use special equipment that operates on unusual frequencies or uses a special type of electromagnetic or optical carrier, spy gear you do not want to be caught with.

7.8 Steganography and Deniability

As you can read, it is all but easy to communicate truly anonymously in today's high-tech and fully digitized world without leaving any traces. Another way to convey the message is to do this openly, but to disguise the message in such a way that no one knows that the message has been sent.

The plaintext message (payload) is encrypted and the ciphertext digits are hidden inside a seemingly innocent text, e-mail or letter (carrier). This technique is called steganography (lit. hidden writing) and enables both sender and receiver to fully deny the existence of encrypted communications. Note that the payload must always be encrypted before hiding it in the carrier. Even when the adversary knows the method of hiding, any attempt to extract encrypted information would merely produce unintelligible digits. The message remains fully deniably. However, an attempt to extract non-encrypted data could reveal the message. Protect before hiding! There are various ways to hide ciphertext digits in a seemingly innocent text. Of course, simply inserting strange sequences of digits or some illogical values will draw suspicion.

The *Words-Per-Sentence* (WPS) system is a simple yet effective method to conceal digits in text. For each digit, a sentence is composed with as many words as the digit + 5 (or any other pre-arranged value). Adding 5 ensures that all sentences have at least five words. Words like "it's", "you're" or "set-up" are regarded as one word. To retrieve the original digits, the receiver simple subtracts 5 from the total number of words in each sentence. To avoid statistical bias, some sentences with less than 5 words or more than 14 words should be added. These are later simply ignored. The advantages of this method are an excellent linguistic freedom and the lack of complex calculations. Always start by writing a meaningful text and then play with the words to obtain the required sentence length. The random digits produce an average of ten-words sentences.

Below, the ciphertext group 68496 from our example message, hidden inside a letter. The receiver counts 11 words in the first sentence and thus knows that the first digit is 11 – 5 = 6.

Dear John,
I Hope everything is going well with you and the family. If possible, Katherine and I would love to visit you somewhere next month. We could make it a weekend at the lake. The next few weeks are rather quiet so any date is fine for us. What do you think? If you're interested, just pick a date and I arrange everything!

Thanks to this system, the hidden message is fully deniable. There is no way to prove the existence of a message inside the innocent looking letter without having the proper one-time pad. We now have a safe method to send encrypted messages covertly by postal mail, e-mail or Internet forums. This is an important advantage in today's digital world where virtually all means to communicate are prone to eavesdropping. Of course, the conversation itself remains detectable and you will need a good excuse for the nonsense you wrote and to whom you wrote it.

7.9 Common Mistakes

To err is human. Unfortunately, mistakes with one-time pads are usually fatal. Below a list of the seven most common mistakes that people make when they use one-time pads.

1. Bad Randomness

The most dangerous error is the use of non-random digits for the key. This is a fatal error you cannot see with the naked eye. Nonetheless, cryptanalysis will discover and exploit this flaw.

2. Not destroying used keys

Humans are collectors. They keep keys that should have been destroyed (the co-called “in case of…” syndrome). Keeping a used key is pointless and dangerous because the message is no longer unbreakable but waiting to be deciphered by those who find the key.

3. Insecure storage of keys

When you store your one-time pads in a five-dollar money box, you will have a five dollar security level. When you store your one-time pads in a real safe, you message is unbreakable if the safe is unbreakable (most safes are not). If you do not securely store or hide your keys, they are compromised from the moment you leave that location.

4. Insecure computers and alike

Computers are a security nightmare and they are never suitable for crypto applications. Everything leaks out and everybody can get in. It is a very common mistake to assume that your computer is secure. It is not, and will never be. It is not because your anti-virus software cannot find anything, that your computer is not infested with spy ware. Modern photocopiers and multi-functional printers have their own processor, store copied documents on their hard disk, and they are usually connected to a network. Do not use those to print or copy confidential information.

5. Multiple copies of a plaintext

If you have stored, processed or sent the unprotected readable plaintext on any type of carrier (computer, USB stick, photocopier, paper…), the message is no longer secure, unless you apply the same strict physical security rules on that carrier as you would apply on your keys. Otherwise, there is a serious risk that the plaintext is compromised, possibly without you even knowing it.

6. Loose lips and false confidence in people

People love secrets, but secrets are only fun when you share them. Loose lips can be fatal. Unbreakable encryption is useless when you tell the secret to others. Humans are unpredictable and you can never know what people do with the information you shared with them. Do not underestimate the primal urge to share secrets! For some people it is almost irresistible. There is a simple yet very effective rule to keep a secret: only share the secret or confidential information on a “need to know” basis. Does he really need to know? If not, do not tell him!

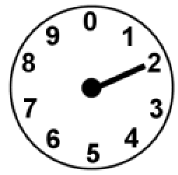
7. Not following the rules

Finally, some people are stubborn and do not follow security rules and advice. They believe they can devise a better or simpler way to do things. They are wrong. They ignore that there are good reasons why all those rules and procedures exist. Do not start improvising to get around seemingly useless, stupid or time-consuming rules.

8. Is One-time Pad Really Unbreakable?

Yes! One-time pad provides perfect secrecy under the following *strict* conditions: all calculations are performed by modular arithmetic, the key is truly random, has the same length as the plaintext, is used only once and destroyed after use. But how can a simple subtraction, addition and modular arithmetic be the basis of truly unbreakable encryption? One-time pad encryption is basically an equation with two unknowns. Now, cryptologists use various statistical and mathematical techniques to guess or estimate those unknowns and use that information to successfully attack the ciphertext. To make that impossible we use one of the most powerful yet simple mathematical tricks of cryptography: the modulo operation. Let us explain this by example.

Let's first use **P + K = C** for encryption, with a normal addition without modulo. Note that P – K = C works just as well (you can swap encryption and decryption operations) but the latter is not as easy to grasp. The values stand for **P**lain, **K**ey and **C**ipher, P and K ranging 0 to 9 and K being random. Although we cannot determine the exact value of P by merely looking at C, we can extract crucial information from C. If C = 0 then we know that both P and K can only be 0. If C = 5 then P and K are either 0 + 5 or 1 + 4 or 2 + 3 or these terms in reversed order. If C = 18 then both P and K can only be 9. Such pieces of information are the golden nuggets for any codebreaker. Anything that confirms or excludes assumptions or possible solutions will always assist in breaking the message. Another inconvenient downside of non-modular arithmetic is that a result that can be a negative value.



Let us now use modular addition, **(P + K) mod 10 = C**. Modular arithmetic works similarly to counting hours, but on a decimal clock. If the hand of our clock is at 7 and we add 4 by advancing clockwise, we pass the 0 and arrive at 1. Likewise, when the clock shows 2 and we subtract 4, advancing anticlockwise, we arrive at 8. It is obvious that, seeing the hand of our clock on a given position, we have no idea where the hand came from, and which two clock positions are added or subtracted. A crucial property of modulo 10 arithmetic is that any sum or difference will always range between 0 and 9, a very convenient property that facilitates manual encryption (for letters A=0 through Z=25 we can use modulo 26, for bits 0-1 we use modulo 2, and for bytes 0-255 modulo 256).

Again, we cannot determine the exact value of P, but, in contrast to normal addition, we cannot exclude or confirm any possible solutions. Indeed, if C = 0 then P and K could be 0 + 0 or 1 + 9 or 2 + 8 or 3 + 7 or 4 + 6 or 5 + 5 or 6 + 4 or 7 + 3 or 8 + 2 or 9 + 1. Likewise, if C = 5 then P and K could be 0 + 5 or 1 + 4 or 2 + 3 or 3 + 2 or 4 + 1 or 5 + 0 or 6 + 9 or 7 + 8 or 8 + 7 or 9 + 6. We can observe that, using modular arithmetic, any value of P is statistically equally possible. Any possible value of C can produce 10 statistically equally likely solutions for P. In other words, with modular arithmetic, it is impossible to find the two unknowns P and K from sum or difference C, and C does not provide any information whatsoever about value P. This is a true equation with two unknowns.

Consequently, each ciphertext digit is completely random and therefore mathematically unrelated to any other digit in that same ciphertext or to its plaintext equivalent. There is also no mathematical relation whatsoever to any other messages because each message uses a new truly random key. These properties, unique to one-time pad, deprive the codebreaker of every possible statistical and mathematical tool to cryptanalyse the ciphertext.

Moreover, the encryption is not based on complex mathematical operations or computational hardness. It is simply mathematically unsolvable, making it invulnerable to any possible future mathematical discoveries or developments in computer technology (computational speed, quantum computing, etc.) One-time pad encryption is therefore what we call information-theoretically secure, *i.e.* unbreakable. Although its concept of perfect secrecy was known since the early 1900s, it was Claude Shannon who presented the mathematical proof in his 1949 paper "Communication Theory of Secrecy Systems", the foundational treatment of modern cryptography.

What if we try out all possible keys, a so-called brute force attack? Will we eventually find the correct solution? Yes, we will. Unfortunately, we would also find many other perfectly readable solutions. Let us demonstrate this with a few examples.

Suppose we intercepted the ciphertext fragment “34818 25667 24857 50594 38586”

Let’s crack the message with the following key: 58472 33602 88472 58584 86707

```
Cipher      34818 25667 24857 50594 38586
Key        +58472 33602 88472 58584 86707
----------------------------------------
Plaincode   82280 58269 02229 08078 14283
```

Converted with our standard checkerboard:

```
R  E  P  O  R  T  fi 222 fi P  L  A  N  E  S
82 2  80 5  82 6  90 222 90 80 78 1  4  2  83
```

The recovered message: **report two planes**

However, there is a second solution with a different key: 58472 33602 81702 57464 98406

```
Cipher      34818 25667 24857 50594 38586
Key        +58472 33602 81702 57464 98606
----------------------------------------
Plaincode   82280 58269 05559 07958 26182
```

```
R  E  P  O  R  T  fi 555 fi M  O  R  T  A  R
82 2  80 5  82 6  90 555 90 79 5  82 6  1  82
```

The recovered message: **report five mortar**

Unfortunately, there is no way to check which key and plaintext are correct. Well, here is the bad news: both solutions are incorrect. The actual message is here below, but we will never know whether this really is the actual message… unless we possess the original key.

```
Cipher      34818 25667 24857 50594 38586
Key        +58472 33605 28941 36331 20507
----------------------------------------
Plaincode   82280 58262 42798 86825 58083
```

```
R  E  P  O  R  T  E  N  E  M  Y  T  R  O  O  P  S
82 2  80 5  82 6  2  4  2  79 88 6  82 5  5  80 83
```

The correct message: **report enemy troops**

These examples show that we can produce any plaintext from any ciphertext, as long as we apply the “proper” wrong key (this also counts for the letters-only version of one-time pad).

Since a series of truly random key digits, mathematically unrelated to each other, determine the plaintext, we have absolutely no idea whether the chosen key is correct. Any readable solution is mathematically and statistically possible and appears valid. There is no way to verify the solution, as it originates from random digits. The system is therefore information-theoretically secure. You have an unbreakable cipher, the only existing, and it will stay unbreakable forever, for everyone.

9. Legal Issues and Personal Security

Cryptography protects the right to privacy and the right to communicate confidentially. Secure communications can protect one's intimate private life, his business relations, and his social or political activities. These basic rights are written in the constitution of many, but not all countries. Of course, it is illegal to use cryptography for criminal or terrorist purposes. This does not mean that the use of cryptography should be illegal. Just as with weapons, a knife or a crowbar, it is not because you could use these objects for illegal purposes that they should be regarded as illegal. It is useless to make cryptography illegal. Criminals simply do not care about the law. If you outlaw cryptography, only outlaws will have privacy.

However, even the most liberal and democratic countries have laws that control the use of cryptography and some countries have stricter laws than others. Many governments are reluctant to permit the use of cryptography by their citizens because it limits the government's surveillance capabilities. The laws are often a balancing between the protection of the individual privacy and a nation's security or its fight against crime.

Democratic countries tend to permit cryptography for personal use and have legal mechanisms to bypass the right to privacy with a court order in case of a criminal investigation or a threat to the nation. The boundary between lawful surveillance and state-organised invasion of privacy is often a subject of discussion, even in democratic countries.

Depending on the country, laws on cryptography can restrict the use of particular crypto algorithms or allow only government licensed systems, limit the strength of the algorithm or its key size, or demand key escrow. Some laws can force people to hand over the decryption keys following a judicial warrant and there are laws that restrict the import or export of cryptographic software, equipment or knowledge, or even regard export of cryptography as weapons export.

Violating these laws can have serious legal consequences, ranging from penalties over prosecution up to imprisonment. In countries with oppressive and dictatorial regimes, democratic rights and laws on privacy are virtually non-existing for ordinary citizens. Such countries usually forbid the use of cryptography to their citizens and the legal consequences can range from long-term imprisonment over torture to death penalty.

Inform yourself about the legal restrictions on cryptography in your country or in the country where you are planning to use it. The use of cryptography, and especially the unbreakable one-time pad system, described in this paper, could result in a criminal investigation, prosecution and severe penalties. In some countries, being caught with one-time pads or sending encrypted messages could cost you your life. Think carefully before you start using one-time pads. It is very easy to encrypt and decrypt messages with one-time pad, but very hard to follow all the necessary strict rules that are vital to protect your and other people's personal security.

The use of one-time pads is always a balance between the protection of your communications and the risks involved in using this system. If you have any doubt about your ability to cope with the security issues or risks involved, do not use encrypted communications!

10.1 Appendix A

Straddling Checkerboards

A practical and efficient method to convert text or into digits is the straddling checkerboard. This is a table with columns and rows, labelled with digits. Column digits that are located above empty top row cells are also used to label the remaining rows. A letter from the top row is converted into a single digit value, designated by its column digit. A letter from the second or third row is converted into a two-digit value, composed by the row and column digits. Allocating the most frequent letters of a language to the top row will reduce the length of the converted text considerably.

Note that a checkerboard does not provide any cryptographic security whatsoever! Therefore, we call the resulting digits a plaincode, to stress that the text is still in its insecure readable form.

The first example, optimised for English, is the simplest version and easily memorised by the mnemonic "AT ONE SIR". Here, T = 1, N = 4, C = 21, J = 26 and W = 64. F/L, represented by 68, switches between letters and figures and / is used as non-mandatory word or sentence separator.

	0	1	2	3	4	5	6	7	8	9
	A	**T**		**O**	**N**	**E**		**S**	**I**	**R**
2	**B**	**C**	**D**	**F**	**G**	**H**	**J**	**K**	**L**	**M**
6	**P**	**Q**	**U**	**V**	**W**	**X**	**Y**	**Z**	**F/L**	**/**

For each additional empty cell in the top row, we can add a full row, thus creating 10 additional cells. The next example, also optimised for English, has four empty cells, allowing four rows of two-digit values. In addition, some cells contain the most frequent English digraphs. Just as the top row letters, these digraphs reduce the total number of digits that are required to convert a text.

CODE 0	A 1	E 2	I 3	O 4	T 5				
AN 60	B 61	C 62	D 63	ED 64	EN 65	ER 66	F 67	G 68	H 69
HA 70	HE 71	IN 72	ION 73	J 74	K 75	L 76	M 77	N 78	ON 79
P 80	Q 81	R 82	RE 83	S 84	TH 85	U 86	V 87	W 88	X 89
Y 90	Z 91	(.) 92	(,) 93	(:) 94	(/) 95	($) 96	(-) 97	F-L 98	SPC 99

Of course, many other tailor-made Checkerboard designs are possible. The goal is always to reduce the message length. The table could contain more trigraphs or even frequently used small words or expressions. Always use combinations that are more efficient than the letters separately (f.i. digraph TO holds no benefit because T and O together also use two digits). You could also allocate both letters and symbols to a single value, controlled by an upper/lower-case cell.

Note that some encryption schemes use checkerboards with scrambled alphabets and/or scrambled labelling. This, however, is not necessary when the conversion is followed by a one-time pad encryption, as this encryption is unbreakable anyway.

Some language and letter frequency optimized checkerboards.

French
(memorized by the keyword SAINTE)

CODE 0	A 1	E 2	I 3	N 4	S 5	T 6	TC NO 1 FRANÇAIS		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
O 80	P 81	Q 82	R 83	U 84	V 85	W 86	X 87	Y 88	Z 89
CHI 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	ESP 99

```
TABLE DE CONVERSION NO.1

CODE-0  B-70  O-80  CHI-90
   A-1  C-71  P-81  (.)-91
   E-2  D-72  Q-82  (:)-92
   I-3  F-73  R-83  (')-93
   N-4  G-74  U-84  ( )-94
   S-5  H-75  V-85  (+)-95
   T-6  J-76  W-86  (-)-96
        K-77  X-87  (=)-97
        L-78  Y-88  REQ-98
        M-79  Z-89  ESP-99
```

German
(memorized by the keyword ANREIS)

CODE 0	A 1	E 2	I 3	N 4	R 5	S 6	UT NR 1 DEUTSCH		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
O 80	P 81	Q 82	T 83	U 84	V 85	W 86	X 87	Y 88	Z 89
ZIF 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	FRG 98	WZR 99

```
UMRECHNUNGSTABELLE NO.1

CODE-0  B-70  O-80  ZIF-90
   A-1  C-71  P-81  (.)-91
   E-2  D-72  Q-82  (:)-92
   I-3  F-73  T-83  (')-93
   N-4  G-74  U-84  ( )-94
   R-5  H-75  V-85  (+)-95
   S-6  J-76  W-86  (-)-96
        K-77  X-87  (=)-97
        L-78  Y-88  FRG-98
        M-79  Z-89  WZR-99
```

Spanish
(memorized by the keyword SENORA)

CODE 0	A 1	E 2	N 3	O 4	R 5	S 6	TC NO 1 ESPAÑOL		
B 70	C 71	D 72	F 73	G 74	H 75	I 76	J 77	K 78	L 79
M 80	P 81	Q 82	T 83	U 84	V 85	W 86	X 87	Y 88	Z 89
CIF 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	ESP 99

```
TABLA DE CONVERCIÓN NO.1

CODE-0  B-70  M-80  CIF-90
   A-1  C-71  P-81  (.)-91
   E-2  D-72  Q-82  (:)-92
   N-3  F-73  T-83  (')-93
   O-4  G-74  U-84  ( )-94
   R-5  H-75  V-85  (+)-95
   S-6  I-76  W-86  (-)-96
        J-77  X-87  (=)-97
        K-78  Y-88  REQ-98
        L-79  Z-89  ESP-99
```

10.2 Appendix B

Printable standard English conversion table and codebook

(memorised by the “ON A TIE” letters, in alphabetic order)

```
CONVERSION TABLE NO.1 (EN)

CODE-0  B-70  P-80  FIG-90
   A-1  C-71  Q-81  (.)-91
   E-2  D-72  R-82  (:)-92
   I-3  F-73  S-83  (')-93
   N-4  G-74  U-84  ( )-94
   O-5  H-75  V-85  (+)-95
   T-6  J-76  W-86  (-)-96
        K-77  X-87  (=)-97
        L-78  Y-88  REQ-98
        M-79  Z-89  SPC-99
```

```
                        CODE TABLE NO.1

000 ABORT       253 DECODE       505 MILITARY    758 STREET
019 ACCEPT      262 DELAY        514 MONEY       767 SUBWAY
028 ACCESS      271 DIFFICULT    523 MONTH       776 SUCCESS
037 ADDRESS     280 DOCUMENT     532 MORNING     785 SUPPLY
046 AFFIRMATIVE 299 ENCODE       541 MORSE       794 SUPPORT
055 AGENT       307 EVENING      550 NEGATIVE    802 TELEPHONE
064 AIRPLANE    316 EXECUTE      569 NIGHT       811 TODAY
073 AIRPORT     325 FACTORY      578 OBSERVATION 820 TOMORROW
082 ANSWER      334 FAILED       587 PASSPORT    839 TRAIN
091 AUTHORITY   343 FERRY        596 PERSON      848 TRANSFER
109 BETWEEN     352 FLIGHT       604 PHOTOGRAPH  857 TRANSMIT
118 BORDER      361 FREQUENCY    613 POSITIVE    866 TRAVEL
127 BUILDING    370 HARBOUR      622 POSSIBLE    875 TRUCK
136 CANCEL      389 HELICOPTER   631 POWER       884 UNABLE TO
145 CHANGE      398 HIGHWAY      640 PRIORITY    893 URGENT
154 CIVILIAN    406 IDENTITY     659 PROBLEM     901 VERIFY
163 COMPROMISE  415 IMMEDIATE    668 QUESTION    910 WEEK
172 COMPUTER    424 IMPOSSIBLE   677 RADIO       929 WITHIN
181 CONFIRM     433 INFORMATION  686 RECEIVE     938 YESTERDAY
190 CONTACT     442 INSTRUCTIONS 695 RENDEZVOUS  947 .........
208 COORDINATE  451 LOCATE       703 REPEAT      956 .........
217 COUNTRY     460 LOCATION     712 RESERVATION 965 .........
226 COVERT      479 MAIL         721 ROUTINE     974 .........
235 CURRENT     488 MEETING      730 SATELLITE   983 .........
244 DANGER      497 MESSAGE      749 SHIP        992 .........
```

10.3 Appendix C

Custom conversion table and codebook

(assign the most frequent characters in your language to digits 1 to 6)

CODE-0	-70	-80	FIG-90
-1	-71	-81	-91
-2	-72	-82	-92
-3	-73	-83	-93
-4	-74	-84	-94
-5	-75	-85	-95
-6	-76	-86	-96
	-77	-87	-97
	-78	-88	-98
	-79	-89	SPC-99

Custom codebook for 100 words or phrases

Three-digit codes with error detection
(each code differs at least two digits from any code)

000	253	505	758
019	262	514	767
028	271	523	776
037	280	532	785
046	299	541	794
055	307	550	802
064	316	569	811
073	325	578	820
082	334	587	839
091	343	596	848
109	352	604	857
118	361	613	866
127	370	622	875
136	389	631	884
145	398	640	893
154	406	659	901
163	415	668	910
172	424	677	929
181	433	686	938
190	442	695	947
208	451	703	956
217	460	712	965
226	479	721	974
235	488	730	983
244	497	749	992

When creating a custom codebook, make sure to select only those words, expression or phrases that would require more than 4 digits if converted separately by the checkerboard.

10.4 Appendix D

Custom codebook for 220 words or phrases

Four-digit codes with error detection
(each code differs at least two digits from any code and no transposition of neighbouring digits)

0000	0594	1582	2790	4675
0011	0660	1595	2882	4686
0022	0671	1661	2893	4697
0033	0682	1670	2992	4774
0044	0693	1683	3333	4785
0055	0770	1692	3342	4796
0066	0781	1771	3351	4884
0077	0792	1780	3360	4895
0088	0880	1793	3377	4994
0099	0891	1881	3386	5555
0110	0990	1890	3395	5564
0121	1111	1991	3443	5577
0132	1120	2222	3452	5586
0143	1133	2233	3461	5591
0154	1142	2240	3470	5665
0165	1155	2251	3487	5674
0176	1164	2266	3496	5687
0187	1177	2277	3553	5696
0198	1186	2284	3562	5775
0220	1199	2295	3571	5784
0231	1221	2332	3580	5797
0242	1230	2343	3597	5885
0253	1243	2350	3663	5894
0264	1252	2361	3672	5995
0275	1265	2376	3681	6666
0286	1274	2387	3690	6677
0297	1287	2394	3773	6684
0330	1296	2442	3782	6695
0341	1331	2453	3791	6776
0352	1340	2460	3883	6787
0363	1353	2471	3892	6794
0374	1362	2486	3993	6886
0385	1375	2497	4444	6897
0396	1384	2552	4455	6996
0440	1397	2563	4466	7777
0451	1441	2570	4477	7786
0462	1450	2581	4480	7795
0473	1463	2596	4491	7887
0484	1472	2662	4554	7896
0495	1485	2673	4565	7997
0550	1494	2680	4576	8888
0561	1551	2691	4587	8899
0572	1560	2772	4590	8998
0583	1573	2783	4664	9999

10.5 Appendix E

Pre-calculated sequence to create a custom codebook for 807 words or phrases

Four-digit codes with error detection
(each code differs at least two digits from any code and no transposition of neighbouring digits)

0000	0550	1166	1718	2305	2936	3521	4114	4681	5354	6038	6600	7231	7849	8583	9217	9933
0011	0564	1177	1732	2316	2949	3534	4123	4705	5367	6042	6611	7240	7854	8591	9229	9944
0022	0589	1188	1746	2324	2980	3545	4131	4737	5370	6050	6622	7256	7868	8601	9246	9955
0033	0605	1199	1769	2332	2992	3553	4140	4742	5402	6061	6633	7273	7876	8612	9258	9966
0044	0616	1202	1771	2347	3003	3568	4157	4756	5410	6074	6644	7282	7887	8630	9263	9977
0055	0624	1210	1780	2351	3014	3576	4162	4761	5421	6104	6655	7294	7903	8643	9274	9988
0066	0637	1221	1793	2360	3025	3587	4185	4774	5434	6116	6666	7315	7914	8654	9281	9999
0077	0648	1234	1808	2373	3031	3607	4203	4783	5445	6125	6677	7329	7926	8668	9295	
0088	0659	1245	1817	2406	3040	3618	4216	4809	5453	6132	6688	7337	7951	8675	9306	
0099	0660	1253	1829	2415	3056	3626	4224	4825	5468	6147	6699	7342	7965	8687	9327	
0102	0671	1267	1836	2423	3062	3632	4232	4858	5476	6151	6701	7350	7978	8696	9339	
0110	0682	1278	1860	2430	3089	3649	4247	4863	5487	6160	6712	7361	7997	8702	9348	
0121	0693	1286	1873	2442	3097	3651	4251	4884	5500	6173	6730	7374	8008	8710	9364	
0134	0708	1303	1881	2457	3105	3663	4260	4892	5511	6205	6748	7383	8017	8721	9371	
0145	0717	1314	1894	2461	3113	3674	4275	4915	5522	6213	6753	7396	8029	8734	9380	
0153	0729	1325	1909	2474	3124	3680	4302	4938	5533	6226	6776	7416	8036	8745	9392	
0167	0736	1331	1928	2489	3130	3695	4310	4959	5544	6237	6787	7438	8064	8759	9408	
0178	0762	1340	1952	2504	3141	3706	4321	4970	5555	6241	6795	7447	8070	8767	9436	
0186	0770	1356	1964	2513	3152	3719	4334	4994	5566	6252	6802	7452	8081	8778	9449	
0201	0781	1362	1975	2526	3169	3727	4345	5005	5577	6264	6810	7460	8093	8786	9485	
0212	0794	1389	1983	2537	3198	3738	4353	5016	5588	6270	6821	7479	8118	8800	9518	
0220	0807	1397	1991	2541	3204	3765	4368	5024	5599	6289	6834	7484	8127	8811	9559	
0235	0818	1404	2002	2552	3215	3773	4376	5032	5604	6309	6845	7491	8139	8822	9561	
0243	0839	1413	2010	2565	3223	3782	4387	5047	5613	6317	6857	7525	8146	8833	9573	
0254	0846	1426	2021	2570	3236	3790	4400	5051	5620	6320	6878	7532	8163	8844	9584	
0268	0861	1437	2034	2598	3242	3816	4411	5060	5639	6336	6886	7548	8171	8855	9596	
0276	0872	1441	2045	2603	3250	3828	4422	5073	5641	6343	6935	7557	8180	8866	9647	
0287	0880	1450	2053	2614	3261	3837	4433	5103	5652	6358	6954	7590	8192	8877	9653	
0304	0895	1465	2067	2625	3279	3859	4444	5115	5665	6372	6967	7602	8207	8888	9669	
0313	0919	1472	2078	2631	3300	3870	4455	5126	5678	6381	6982	7610	8228	8899	9676	
0326	0927	1498	2086	2640	3311	3883	4466	5137	5686	6394	6996	7621	8249	8904	9694	
0330	0956	1505	2101	2656	3322	3891	4477	5142	5697	6407	7007	7634	8265	8913	9704	
0341	0973	1516	2112	2662	3333	3908	4488	5150	5731	6418	7018	7645	8272	8925	9713	
0352	0984	1524	2120	2679	3344	3917	4499	5161	5740	6424	7039	7658	8284	8932	9720	
0365	0990	1530	2135	2709	3355	3929	4501	5174	5758	6431	7046	7667	8290	8941	9735	
0379	1001	1547	2143	2728	3366	3946	4512	5189	5764	6446	7063	7689	8338	8950	9741	
0398	1012	1551	2154	2763	3377	3960	4520	5206	5775	6459	7071	7700	8357	8976	9752	
0403	1020	1563	2168	2772	3388	3972	4535	5214	5792	6462	7080	7711	8369	8998	9768	
0414	1035	1579	2176	2784	3399	3985	4543	5225	5843	6475	7092	7722	8382	9009	9779	
0425	1043	1582	2187	2791	3401	3993	4554	5230	5856	6480	7109	7733	8395	9028	9805	
0432	1054	1606	2200	2819	3412	4004	4567	5248	5869	6493	7117	7744	8405	9037	9814	
0440	1068	1615	2211	2827	3420	4013	4578	5257	5885	6503	7128	7755	8419	9072	9823	
0451	1076	1623	2222	2838	3435	4026	4586	5262	5890	6514	7136	7766	8448	9083	9831	
0469	1087	1638	2233	2850	3443	4030	4608	5271	5963	6527	7164	7777	8456	9091	9840	
0497	1100	1642	2244	2864	3454	4041	4617	5283	5979	6540	7170	7788	8473	9107	9862	
0506	1111	1657	2255	2871	3467	4052	4629	5301	5981	6556	7181	7799	8494	9119	9889	
0515	1122	1661	2266	2882	3478	4065	4636	5312	5995	6569	7195	7801	8509	9138	9897	
0523	1133	1670	2277	2893	3486	4079	4650	5323	6006	6571	7208	7812	8558	9156	9900	
0531	1144	1684	2288	2907	3502	4098	4664	5335	6015	6585	7219	7820	8560	9182	9911	
0542	1155	1707	2299	2918	3510	4106	4672	5346	6023	6592	7227	7835	8574	9190	9922	

10.6 Appendix F

Morse Cut Numbers

Various cut numbers systems to shorten the transmission time of Morse digits

Morse Full Numbers		Morse Cut Numbers									
		Standard Short		International		CIS 1		CIS 2		Cuban	
1	·----	1	·- (A)	1	·- (A)	1	·- (A)	1	·- (A)	1	·- (A)
2	··---	2	··- (U)	2	··- (U)	2	-··· (B)	2	·-- (W)	2	-· (N)
3	···--	3	···- (V)	3	·-- (W)	3	·-- (W)	3	· (E)	3	-·· (D)
4	····-	4	····- (4)	4	···- (V)	4	--· (G)	4	·-· (R)	4	··- (U)
5	·····	5	· (E)	5	··· (S)	5	-·· (D)	5	- (T)	5	·-- (W)
6	-····	6	-···· (6)	6	-··· (B)	6	· (E)	6	-·-- (Y)	6	·-· (R)
7	--···	7	-··· (B)	7	--· (G)	7	···- (V)	7	··- (U)	7	·· (I)
8	---··	8	-·· (D)	8	-·· (D)	8	--·· (Z)	8	·· (I)	8	--· (G)
9	----·	9	-· (N)	9	-· (N)	9	·· (I)	9	--- (O)	9	-- (M)
0	-----	0	- (T)	0	- (T)	0	-·- (K)	0	·--· (P)	0	- (T)

10.7 Appendix G

A Brief History of One-time Pad

In 1882, Californian banker Frank Miller developed cipher system which is now regarded as the first know application of one-time pad. He compiled a telegraphic code book to compresses 14,000 words and phrases into short number-codes. For additional security, he added secret key numbers to these codes to produce a ciphertext. If the sum exceeded 14,000, one had to subtract 14,000 from the sum. To decrypt the message, one had to subtract the secret number from the ciphertext. If that result would be smaller than 0, one had to add 14,000 to the ciphertext before subtraction. This is actually a modulo 14,000 arithmetic. He described the key numbers as a list of irregular numbers that should never be re-used. It's the first description of one-time pad. Unfortunately, Miller's perfect cipher, and its potential, never became generally known. It got lost in the history of cryptography and disappeared in oblivion, only to be rediscovered in archives in 2011.

In 1917, AT&T research engineer Gilbert Vernam developed a system to encrypt teletype TTY communications. Vernam mixed a five-bit punched paper tape, containing the message, with a second punched paper tape, the key, containing random five-bit values. A system of relays performed a modulo 2 addition (later known as XOR) to mix the bits of the two punched tapes. The key tape ran synchronously on the sending and receiving teletype machine. It was the first automated instant on-line encryption system. Soon after, U.S. Captain Joseph Mauborgne correctly concluded that the message would be perfectly secure if the key tape was completely unpredictable and never re-used. One-time encryption was reborn.

AT&T marketed the Vernam system in the 1920's for commercial secure communications, albeit with little success. The production, distribution and consumption of enormous quantities of one-time tapes limited its use to fixed stations like headquarters or communications centers. It was not until the Second World War that the U.S. Signal Corps widely used the OTT system for its high-level teleprinter communications.

However, three German cryptologists, Werner Kunze, Rudolf Schauffler and Erich Langlotz, did immediately recognise the advantages of one-time encryption in the early 1920's. While cryptanalysing French diplomatic traffic - a short repetitive numerical key added modulo 10 to codebook numbers - they realised that adding unique random numbers to each code group would make the message unbreakable. They devised a system with paper sheets containing random numbers of which there were only two copies that had to be destroyed after use. In fact, they re-invented Frank Miller's 1882 system.

By 1923, the system was introduced in the German foreign office to protect their diplomatic correspondence. For the first time in history, diplomats had truly unbreakable encryption at their disposal. Later on, many variations on this pencil-and-paper system were devised. The name one-time pad or OTP refers to small notepads with random digits or letters. For each new message, a new sheet is torn off. This pencil and paper version of the one-time pad later became popular very with intelligence agencies.

In 1943, the letters-based one-time pad became the main cipher of the British Special Operations Executive (SOE) to replace insecure poem based transposition ciphers and book ciphers. The system was used extensively during and after the Second World War by many intelligence organisations, sabotage and espionage units. The unbreakable encryption protects operatives and their contacts against decryption of their communications and disclosure of their identities. Such level of security cannot be guaranteed with other encryption systems during long-running operations because the opponent might eventually have enough time or computer power to successfully decrypt the messages.

Soviet Intelligence and military historically always relied heavily on one-time pad encryption, and for good reason. Their communications have always proved extremely secure during WW2 and the Cold War. A common misconception is that the Cold War codebreaking project VENONA cracked Soviet KGB and GRU one-time pads. In reality, they never broke the actually encryption but exploited re-used keys, a fatal flaw, caused by erroneous distribution of more than two copies of certain keys by the Soviets.

One-time pads were widely used by Foreign Service communicators until the 1980's, usually in combination with codebooks containing all kinds of words or phrases, represented by a short number-code. These codebooks were designed to reduce the message length for transmission over commercial cable or telex and were valid for a long period of time, which didn't affect security, as the messages were one-time pad encrypted anyway.

Machines using one-time tapes (OTT) remained very popular for many decades, because of their absolute security, unequalled by any other crypto machine or algorithm. A most famous example is the Washington-Moscow hotline with the ETCRRM II, a standard commercial one-time tape mixer for Telex machines (the hotline was never a red telephone, as erroneous portrayed in popular media). Although simple and cheap, the ETCRRM provided unbreakable communications between Washington and the Kremlin, without disclosing any secret crypto technology to the adversary.

Some other cipher machines that used the principle of one-time pad were the American TELEKRYPTON, SIGSALY (noise as one-time pad), B-2 PYTHON and SIGTOT, the British BID-590 NOREEN and 5-UCO, the Canadian ROCKEX, the Dutch ECOLEX series, the German Siemens T-37-ICA and M-190, the East German T-304 LEGUAN, the Czech SD1, the Russian M-100 SMARAGD and M-105 N AGAT and the Polish T-352/T-353 DUDEK.

A unique advantage of the punched tape keys was that copying them quickly was virtually impossible as the sealed plastic bag with its reel of punched tape had printed serial numbers and other markings on its side. To unwind the tape, copy it and rewind it again with a perfectly aligned print, at the scene of the crime, was virtually impossible. Therefore, they were more secure than key list sheets with short keys, generally used for conventional ciphering machines, which are copied quickly by hand or by taking a photo.

Today, digital versions of the one-time pad enable the storage of huge quantities of random key data, allowing encryption of large volumes of computer data. This absolutely secure encryption is interesting for top-level communications within governments, intelligence and military.

However, even today, pencil-and-paper versions still find their use in covert communications. One well-known example are numbers stations, broadcasting streams of numbers messages to operatives the field. It's an perfectly secure system to receive operational orders. We know this from historical archives, but also from very recent spy cases. The spies were caught while they were flagged for various other reasons, but seized pads or deciphered message eventually provided additional evidence for their spying activities.

One-time encryption still is, and will continue to be, the only system that can offer absolute message secrecy. In the end, even the brightest codebreakers from the best intelligence agencies, using the most advanced mathematics, with infinite computer power and time at their disposal will never succeed in breaking one-time pad, because it is simply mathematically impossible.

Please visit the Cipher Machines and Cryptology website for more information and images.

http://users.telenet.be/d.rijmenants/en/onetimepad.htm